ID: 512648
Sample Name: V2WzER53Tt
Cookbook:
defaultlinuxfilecookbook.jbs
Time: 09:42:44
Date: 01/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

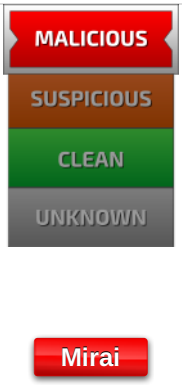
Linux Analysis Report V2WzER53Tt

Overview

General Information

Sample Name:	V2WzER53Tt
Analysis ID:	512648
MD5:	4b0259083c8800..
SHA1:	f58aa2b92704774.
SHA256:	7feef5ad07bad63..
Tags:	32 elf intel mirai
Infos:	

Detection

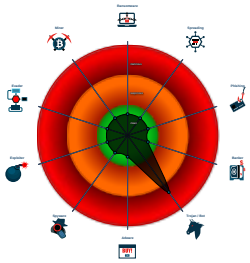


Score:	72
Range:	0 - 100
Whitelisted:	false

Signatures

- Snort IDS alert for network traffic (e....
- Yara detected Mirai
- Multi AV Scanner detection for subm...
- Uses known network protocols on no...
- Machine Learning detection for samp...
- Yara signature match
- Sample has stripped symbol table
- Enumerates processes within the "p...
- Tries to connect to HTTP servers, b...
- Detected TCP or UDP traffic on non...

Classification



Analysis Advice

All HTTP servers contacted by the sample do not answer. Likely the sample is an old dropper which does no longer work

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	512648
Start date:	01.11.2021
Start time:	09:42:44
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	V2WzER53Tt
Cookbook file name:	defaultlinuxfilecookbook.jbs
Analysis system description:	Ubuntu Linux 20.04 x64 (Kernel 5.4.0-72, Firefox 91.0, Evince Document Viewer 3.36.10, LibreOffice 6.4.7.2, OpenJDK 11.0.11)
Analysis Mode:	default
Detection:	MAL
Classification:	mal72.troj.lin@0/0@1/0
Warnings:	Show All

Process Tree

- **system is lnxubuntu20**
- V2WzER53Tt (PID: 5240, Parent: 5115, MD5: 4b0259083c8800d18cb941c66639a2e6) Arguments: /tmp/V2WzER53Tt
  - V2WzER53Tt New Fork (PID: 5241, Parent: 5240)
  - V2WzER53Tt New Fork (PID: 5242, Parent: 5240)
    - V2WzER53Tt New Fork (PID: 5243, Parent: 5242)
    - V2WzER53Tt New Fork (PID: 5244, Parent: 5242)
    - V2WzER53Tt New Fork (PID: 5245, Parent: 5242)
- **cleanup**

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
V2WzER53Tt	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x10ba8:$xo1: Dfs`eeh&<'9 • 0x10c20:$xo1: Dfs`eeh&<'9 • 0x10c94:$xo1: Dfs`eeh&<'9 • 0x10d04:$xo1: Dfs`eeh&<'9 • 0x10d50:$xo1: Dfs`eeh&<'9

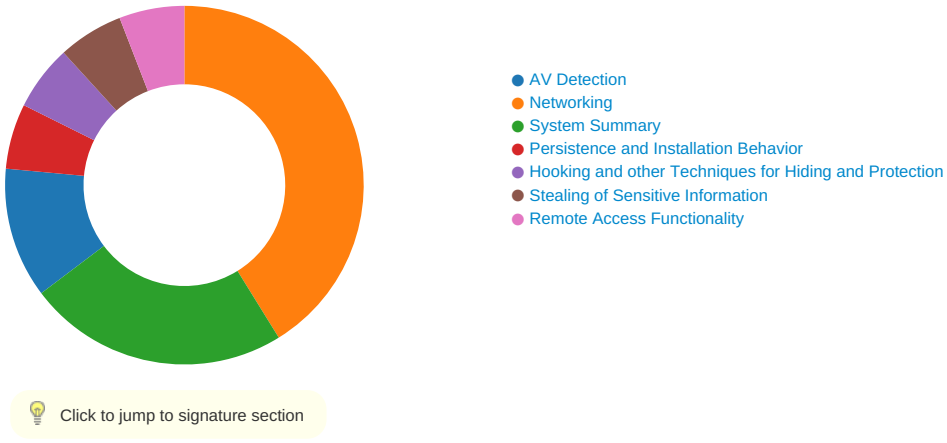
PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_Mirai_12	Yara detected Mirai	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
5241.1.000000007fd4a080.0000000002b07ef2.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x6d0:$xo1: Dfs`eeh&<'9 • 0x750:$xo1: Dfs`eeh&<'9 • 0x7c8:$xo1: Dfs`eeh&<'9 • 0x840:$xo1: Dfs`eeh&<'9 • 0x890:$xo1: Dfs`eeh&<'9
5240.1.000000001a887bdc.0000000019a04c35.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x10ba8:$xo1: Dfs`eeh&<'9 • 0x10c20:$xo1: Dfs`eeh&<'9 • 0x10c94:$xo1: Dfs`eeh&<'9 • 0x10d04:$xo1: Dfs`eeh&<'9 • 0x10d50:$xo1: Dfs`eeh&<'9
5243.1.000000007fd4a080.0000000002b07ef2.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x6d0:$xo1: Dfs`eeh&<'9 • 0x750:$xo1: Dfs`eeh&<'9 • 0x7c8:$xo1: Dfs`eeh&<'9 • 0x840:$xo1: Dfs`eeh&<'9 • 0x890:$xo1: Dfs`eeh&<'9
5243.1.000000001a887bdc.0000000019a04c35.r-x.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x10ba8:$xo1: Dfs`eeh&<'9 • 0x10c20:$xo1: Dfs`eeh&<'9 • 0x10c94:$xo1: Dfs`eeh&<'9 • 0x10d04:$xo1: Dfs`eeh&<'9 • 0x10d50:$xo1: Dfs`eeh&<'9
5240.1.000000007fd4a080.0000000002b07ef2.rw-.sdmp	SUSP_XORed_Mozilla	Detects suspicious XORed keyword - Mozilla/5.0	Florian Roth	• 0x6d0:$xo1: Dfs`eeh&<'9 • 0x750:$xo1: Dfs`eeh&<'9 • 0x7c8:$xo1: Dfs`eeh&<'9 • 0x840:$xo1: Dfs`eeh&<'9 • 0x890:$xo1: Dfs`eeh&<'9
Click to see the 1 entries				

Jbx Signature Overview



AV Detection:

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

Uses known network protocols on non-standard ports

Hooking and other Techniques for Hiding and Protection:

Uses known network protocols on non-standard ports

Stealing of Sensitive Information:

Yara detected Mirai

Remote Access Functionality:

Yara detected Mirai

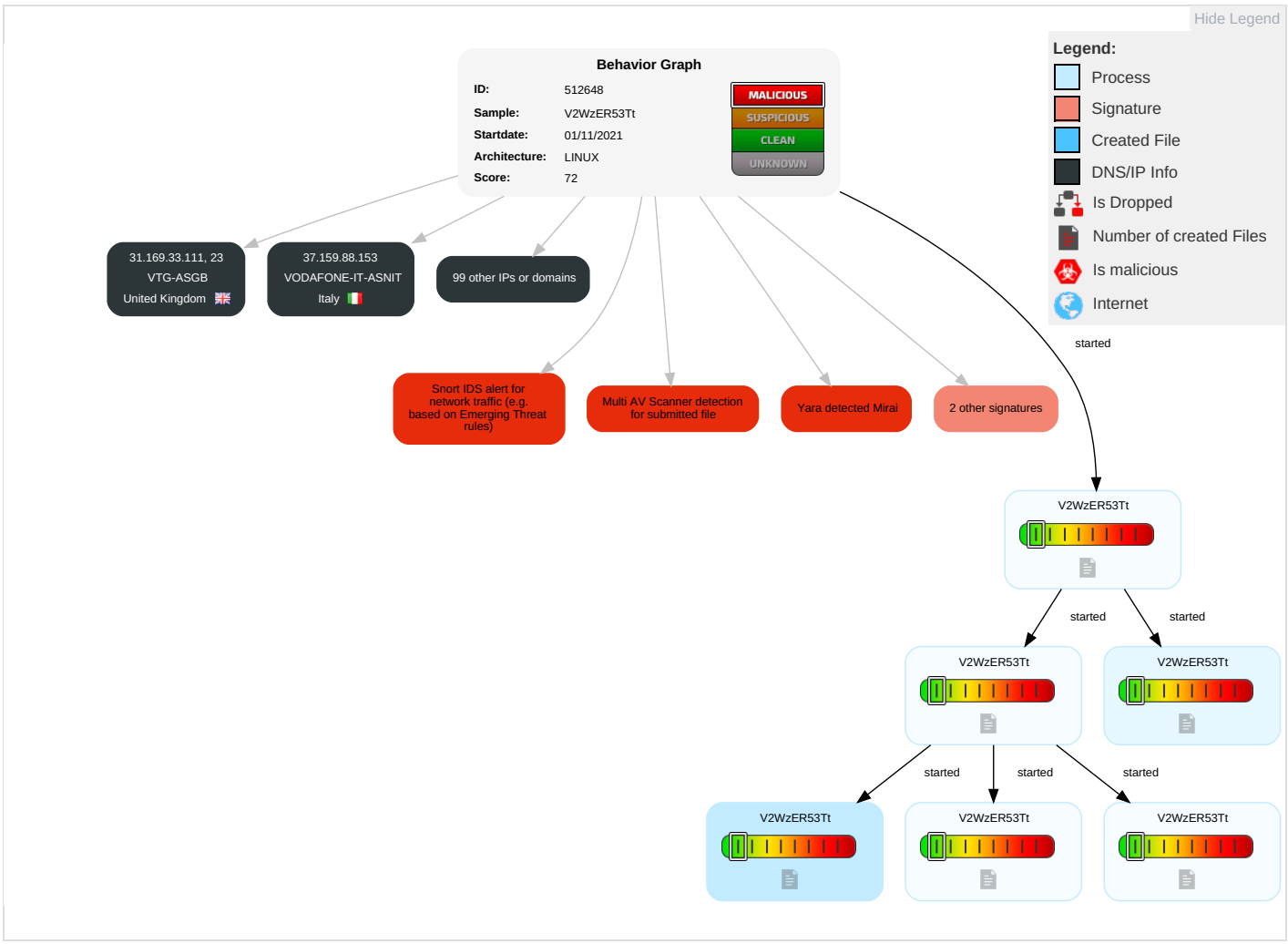
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	Path Interception	Direct Volume Access	OS Credential Dumping 1	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Application Window Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1 1	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	Query Registry	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	System Network Configuration Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 2	SIM Card Swap		Carrier Billing Fraud

Malware Configuration

No configs have been found

Behavior Graph



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
V2WzER53Tt	32%	Virustotal		Browse
V2WzER53Tt	40%	ReversingLabs	Linux.Trojan.Mirai	
V2WzER53Tt	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
z0x3n.cf	37.0.10.67	true	false		unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
72.61.165.33	unknown	United States		10507	SPCSUS	false
174.231.28.33	unknown	United States		22394	CELLCOUS	false
39.24.241.136	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	false
80.182.138.23	unknown	Italy		3269	ASN-IBSNAZIT	false
204.251.17.168	unknown	United States		22713	CAC-HQ2US	false
219.172.230.13	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
126.124.161.79	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	false
37.136.71.101	unknown	Finland		16086	DNAFI	false
138.209.196.84	unknown	United States		21727	HAMLINE-EDUUS	false
43.241.121.32	unknown	India		134033	HIREACH-BROADBAND-ASHIREACHBROADBANDPRIVATELTDIN	false
54.44.16.34	unknown	United States		14618	AMAZON-AESUS	false
80.169.192.37	unknown	United Kingdom		8220	COLTCOLTTechnologyServicesGroupLimitedGB	false
181.211.64.123	unknown	Ecuador		28006	CORPORACIONNACIONALDETELECOMUNICACIONES-CNTEPEC	false
70.59.57.90	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
43.95.13.184	unknown	Japan		4249	LILLY-ASUS	false
182.227.223.141	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	false
4.44.140.137	unknown	United States		3356	LEVEL3US	false
196.127.145.120	unknown	Morocco		36925	ASMediMA	false
17.116.204.52	unknown	United States		714	APPLE-ENGINEERINGUS	false
38.52.8.233	unknown	United States		174	COGENT-174US	false
105.151.162.125	unknown	Morocco		6713	IAM-ASMA	false
51.0.250.204	unknown	United Kingdom		2686	ATGS-MMD-ASUS	false
45.254.230.231	unknown	China		132116	ANINETWORK-INAniNetworkPvtLtdIN	false
41.123.244.87	unknown	South Africa		16637	MTNNS-ASZA	false
195.6.129.86	unknown	France		3215	FranceTelecom-OrangeFR	false
58.219.212.189	unknown	China		134769	CHINANET-JIANGSU-CHANGZHOU-IDCChinaNetJiangsuChangzhouID	false
175.75.234.174	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
153.157.16.253	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
64.26.154.152	unknown	Canada		812	ROGERS-COMMUNICATIONSCA	false
69.119.10.251	unknown	United States		6128	CABLE-NET-1US	false
39.89.3.190	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
37.159.88.153	unknown	Italy		30722	VODAFONE-IT-ASNIT	false
216.8.206.18	unknown	United States		8008	ETC-60-ASUS	false
112.98.49.112	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
19.129.23.236	unknown	United States		3	MIT-GATEWAYSUS	false
73.174.67.125	unknown	United States		7922	COMCAST-7922US	false
48.227.10.242	unknown	United States		2686	ATGS-MMD-ASUS	false
112.85.157.26	unknown	China		4837	CHINA169-BACKBONECHINAUNICOMChina169BackboneCN	false
212.103.208.192	unknown	Italy		12481	TRIVENETTELECOMUNICAZIONIIT	false
185.247.249.224	unknown	France		16347	RMI-FITECHFR	false
95.69.98.131	unknown	Portugal		42863	MEO-MOVELPT	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
180.205.175.239	unknown	Taiwan; Republic of China (ROC)		24158	TAIWANMOBILE-ASTaiwanMobileCoLtdTW	false
193.7.233.94	unknown	Germany		12680	GRUNER-UND-JAHR-AS1HamburgGermanyDE	false
186.121.83.11	unknown	Colombia		28118	ALTICEDOMINICANASADO	false
38.148.28.63	unknown	United States		174	COGENT-174US	false
115.202.233.11	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
80.71.44.37	unknown	Canada		395965	CARRY-TELECOMCA	false
46.34.19.139	unknown	United Kingdom		8190	MDNXGB	false
150.4.28.217	unknown	Japan		6400	CompaniaDominicanadeTelefonosSADO	false
92.228.85.84	unknown	Germany		6805	TDDE-ASN1DE	false
153.198.14.200	unknown	Japan		4713	OCNNTTCommunicationsCorporationJP	false
45.174.220.33	unknown	Brazil		268869	FIBRAPLUSTELECOMUNICACOESLTDAEPPBR	false
201.209.195.191	unknown	Venezuela		8048	CANTVServiciosVenezuelaVE	false
54.140.16.174	unknown	United States		14618	AMAZON-AESUS	false
83.82.205.155	unknown	Netherlands		33915	TNF-ASNL	false
62.34.235.245	unknown	France		5410	BOUYGTEL-ISPFR	false
109.52.47.222	unknown	Italy		16232	ASN-TIMServiceProviderIT	false
91.105.101.213	unknown	Latvia		12578	APOLLO-ASLatviaLV	false
103.71.132.236	unknown	Singapore		45062	NETEASE-ASGuangzhouNetEaseComputerSystemCoLtdCN	false
24.95.244.76	unknown	United States		33363	BHN-33363US	false
201.99.236.86	unknown	Mexico		8151	UninetSAdeCVMX	false
174.174.228.191	unknown	United States		7922	COMCAST-7922US	false
206.101.65.213	unknown	United States		7991	CENTURYLINK-LEGACY-SAVVIS-ASIA-TRANSITUS	false
110.135.70.133	unknown	Japan		9824	JTCL-JP-ASJupiterTelecommunicationCoLtdJP	false
201.218.134.124	unknown	Chile		52439	OPTICCL	false
161.51.59.122	unknown	United States		16525	KBRUS	false
81.177.17.65	unknown	Russian Federation		8342	RTCOMM-ASRU	false
141.70.176.199	unknown	Germany		553	BELWUEBelWue-KoordinationEU	false
48.172.161.127	unknown	United States		2686	ATGS-MMD-ASUS	false
206.106.173.7	unknown	United States		1239	SPRINTLINKUS	false
204.98.5.51	unknown	United States		209	CENTURYLINK-US-LEGACY-QWESTUS	false
40.1.113.122	unknown	United States		4249	LILLY-ASUS	false
142.84.38.207	unknown	Canada		11489	BACICA	false
78.111.77.240	unknown	Germany		33984	SURFPLANET-ASDE	false
196.86.138.209	unknown	Morocco		6713	IAM-ASMA	false
107.185.34.158	unknown	United States		20001	TWC-20001-PACWESTUS	false
124.225.246.124	unknown	China		4134	CHINANET-BACKBONENo31Jin-rongStreetCN	false
176.50.235.57	unknown	Russian Federation		12389	ROSTELECOM-ASRU	false
61.89.86.94	unknown	Japan		18081	KCNKintetsuCableNetworkCoLtdJP	false
175.85.234.246	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
210.69.66.11	unknown	Taiwan; Republic of China (ROC)		4782	GSNETDataCommunicationBusinessGroupTW	false
160.87.222.141	unknown	United States		299	UCINET-ASUS	false
19.207.207.91	unknown	United States		3	MIT-GATEWAYSUS	false
37.155.95.200	unknown	Turkey		20978	TT_MOBILIstanbulTR	false
35.82.186.28	unknown	United States		237	MERIT-AS-14US	false
145.82.121.128	unknown	Saudi Arabia		1103	SURFNET-NLSURFnetTheNetherlandsNL	false
19.21.250.153	unknown	United States		3	MIT-GATEWAYSUS	false
108.29.81.107	unknown	United States		701	UUNETUS	false

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
110.63.108.249	unknown	China		9394	CTTNETChinaTieTongTelecommunicationsCorporationCN	false
32.105.99.166	unknown	United States		2688	ATGS-MMD-ASUS	false
146.87.199.178	unknown	United Kingdom		786	JANETJiscServicesLimitedGB	false
82.32.160.125	unknown	United Kingdom		5089	NTLGB	false
164.150.162.231	unknown	South Africa		37130	SITA-ASZA	false
206.176.163.168	unknown	United States		18818	LSUHSCS-NET2US	false
31.169.33.111	unknown	United Kingdom		60194	VTG-ASGB	false
74.166.99.108	unknown	United States		7018	ATT-INTERNET4US	false
207.177.239.150	unknown	United States		7735	REDSHIFTUS	false
159.222.210.23	unknown	United States		26395	JOHNSON-CONTROLSUS	false
200.183.188.183	unknown	Brazil		4230	CLAROSABR	false
4.143.28.65	unknown	United States		3356	LEVEL3US	false

Runtime Messages

Command:	/tmp/V2WzER53Tt
Exit Code:	0
Exit Code Info:	
Killed:	False
Standard Output:	0G0dn3t Got To Ya!
Standard Error:	

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
58.219.212.189	jew.arm7	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
z0x3n.cf	1bL17EUgTk	Get hash	malicious	Browse	• 37.0.10.67
	pTF1ilCUEm	Get hash	malicious	Browse	• 37.0.10.67
	z0x3n.arm7	Get hash	malicious	Browse	• 37.0.10.67
	z0x3n.x86	Get hash	malicious	Browse	• 37.0.10.67

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
SPCSUS	032k4JmR0U	Get hash	malicious	Browse	• 108.113.255.159
	arm	Get hash	malicious	Browse	• 173.135.71.137
	x86	Get hash	malicious	Browse	• 70.9.116.82
	arm7	Get hash	malicious	Browse	• 68.26.166.237
	z0x3n.arm7	Get hash	malicious	Browse	• 108.124.110.113
	z0x3n.x86	Get hash	malicious	Browse	• 72.59.167.134
	arm	Get hash	malicious	Browse	• 174.151.241.175
	QtNnZoNz75	Get hash	malicious	Browse	• 184.207.33.128
	S13B4aCa4E	Get hash	malicious	Browse	• 184.209.111.81
	gbk4XWulUo	Get hash	malicious	Browse	• 184.205.51.89
	QZ2CN6CUyv	Get hash	malicious	Browse	• 184.251.25.180
	8MPbeDAwwZ	Get hash	malicious	Browse	• 184.243.41.199
	HgTC70XRum	Get hash	malicious	Browse	• 184.239.67.225

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Xs0PMn85CN	Get hash	malicious	Browse	• 108.110.174.155
	Tsunami.x86	Get hash	malicious	Browse	• 184.223.137.41
	Tsunami.arm7	Get hash	malicious	Browse	• 184.253.108.231
	Tsunami.arm	Get hash	malicious	Browse	• 184.245.8.26
	x86	Get hash	malicious	Browse	• 184.216.124.79
	KXAJjgoH22	Get hash	malicious	Browse	• 173.152.132.234
	0r73kbzSGC	Get hash	malicious	Browse	• 184.192.179.21
CELLCOUS	a5nulABeSk	Get hash	malicious	Browse	• 72.109.28.224
	032k4JmR0U	Get hash	malicious	Browse	• 97.45.108.79
	arm	Get hash	malicious	Browse	• 70.221.126.72
	x86	Get hash	malicious	Browse	• 166.159.16.21
	z0x3n.arm7	Get hash	malicious	Browse	• 75.235.188.204
	QZ2CN6CUyv	Get hash	malicious	Browse	• 97.56.241.131
	x86	Get hash	malicious	Browse	• 174.219.17.232
	arm7	Get hash	malicious	Browse	• 174.237.27.157
	WnhlYWJ5C5	Get hash	malicious	Browse	• 72.127.172.19
	dqnskKAmQq	Get hash	malicious	Browse	• 72.104.231.57
	jJ6GK5qbZt	Get hash	malicious	Browse	• 166.145.186.136
	x86	Get hash	malicious	Browse	• 166.239.43.208
	JUZVpUSH0W	Get hash	malicious	Browse	• 174.239.100.9
	07xBxVsvEn	Get hash	malicious	Browse	• 166.140.14.127
	5mLAGfiGBf	Get hash	malicious	Browse	• 72.115.215.214
	wannacry.exe	Get hash	malicious	Browse	• 72.105.156.213
	wTFR3LK4Mo	Get hash	malicious	Browse	• 174.192.243.230
	yZ7D7o1Z7p	Get hash	malicious	Browse	• 70.201.163.147
	eNrYzJWFvB	Get hash	malicious	Browse	• 166.161.44.184
	IcwrPqGkXP	Get hash	malicious	Browse	• 72.113.124.144

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	ELF 32-bit LSB executable, Intel 80386, version 1 (SYSV), statically linked, stripped
Entropy (8bit):	6.203678716949746
TrID:	• ELF Executable and Linkable format (Linux) (4029/14) 50.16% • ELF Executable and Linkable format (generic) (4004/1) 49.84%
File name:	V2WzER53Tt
File size:	71312
MD5:	4b0259083c8800d18cb941c66639a2e6
SHA1:	f58aa2b927047749395a47b16b458f5220d19f3a

General

SHA256:	7feef5ad07bad632f6440d1fb5e0aaf9464fe27eb7ea5e489ae4f79bfee5b2ea
SHA512:	d72d40832e31803a73d1615ffc6eb6b6e046d36afac6cb1d4462b3dc50dd5a8ebce10c5ba4d44fb4fad8f6760167d3c219fecfe6c65359d07226b8e1199555d7
SSDEEP:	1536:bWscjmrfvWdHCX9hGnYtWQgJIY3pp6mqOj:bWirfvWxCXGYtFcpImH
File Content Preview:	.ELF.....h...4.....4. ...(.....`..`.....d...d...d..\...\.....Q.td.....U..S.....".h.....[]...$.....U.....=.....t..1.....u.....t...$`.....

Static ELF Info

ELF header

Class:	ELF32
Data:	2's complement, little endian
Version:	1 (current)
Machine:	Intel 80386
Version Number:	0x1
Type:	EXEC (Executable file)
OS/ABI:	UNIX - System V
ABI Version:	0
Entry Point Address:	0x8048168
Flags:	0x0
ELF Header Size:	52
Program Header Offset:	52
Program Header Size:	32
Number of Program Headers:	3
Section Header Offset:	70912
Section Header Size:	40
Number of Section Headers:	10
Header String Table Index:	9

Sections

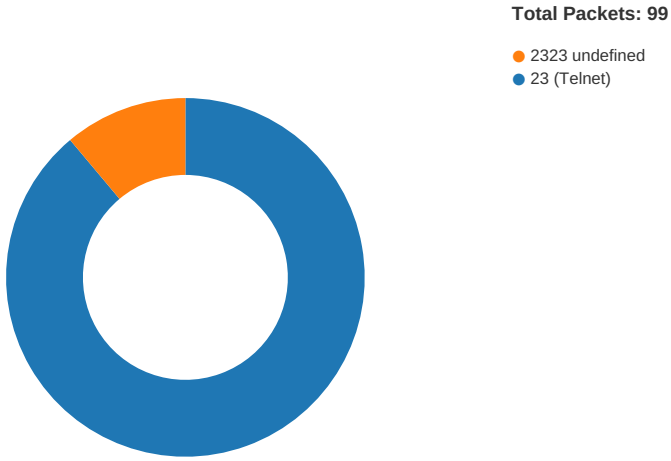
Name	Type	Address	Offset	Size	EntSize	Flags	Flags Description	Link	Info	Align
	NULL	0x0	0x0	0x0	0x0	0x0		0	0	0
.init	PROGBITS	0x8048094	0x94	0x1c	0x0	0x6	AX	0	0	1
.text	PROGBITS	0x80480b0	0xb0	0x10401	0x0	0x6	AX	0	0	16
.fini	PROGBITS	0x80584b1	0x104b1	0x17	0x0	0x6	AX	0	0	1
.rodata	PROGBITS	0x80584e0	0x104e0	0xe80	0x0	0x2	A	0	0	32
.ctors	PROGBITS	0x805a364	0x11364	0x8	0x0	0x3	WA	0	0	4
.dtors	PROGBITS	0x805a36c	0x1136c	0x8	0x0	0x3	WA	0	0	4
.data	PROGBITS	0x805a3a0	0x113a0	0x120	0x0	0x3	WA	0	0	32
.bss	NOBITS	0x805a4c0	0x114c0	0x800	0x0	0x3	WA	0	0	32
.shstrtab	STRTAB	0x0	0x114c0	0x3e	0x0	0x0		0	0	1

Program Segments

Type	Offset	Virtual Address	Physical Address	File Size	Memory Size	Entropy	Flags	Flags Description	Align	Prog Interpreter	Section Mappings
LOAD	0x0	0x8048000	0x8048000	0x11360	0x11360	3.5001	0x5	R E	0x1000		.init .text .fini .rodata
LOAD	0x11364	0x805a364	0x805a364	0x15c	0x95c	2.4364	0x6	RW	0x1000		.ctors .dtors .data .bss
GNU_STACK	0x0	0x0	0x0	0x0	0x0	0.0000	0x6	RW	0x4		

Network Behavior

Network Port Distribution



TCP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 1, 2021 09:43:28.390194893 CET	192.168.2.23	8.8.8.8	0x4f2d	Standard query (0)	z0x3n.cf	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 1, 2021 09:43:28.426201105 CET	8.8.8.8	192.168.2.23	0x4f2d	No error (0)	z0x3n.cf		37.0.10.67	A (IP address)	IN (0x0001)

System Behavior

Analysis Process: V2WzER53Tt PID: 5240 Parent PID: 5115

General

Start time:	09:43:27
Start date:	01/11/2021
Path:	/tmp/V2WzER53Tt
Arguments:	/tmp/V2WzER53Tt
File size:	71312 bytes
MD5 hash:	4b0259083c8800d18cb941c66639a2e6

Analysis Process: V2WzER53Tt PID: 5241 Parent PID: 5240

General

Start time:	09:43:27
Start date:	01/11/2021
Path:	/tmp/V2WzER53Tt
Arguments:	n/a
File size:	71312 bytes
MD5 hash:	4b0259083c8800d18cb941c66639a2e6

Analysis Process: V2WzER53Tt PID: 5242 Parent PID: 5240

General

Start time:	09:43:27
Start date:	01/11/2021
Path:	/tmp/V2WzER53Tt
Arguments:	n/a
File size:	71312 bytes
MD5 hash:	4b0259083c8800d18cb941c66639a2e6

Analysis Process: V2WzER53Tt PID: 5243 Parent PID: 5242

General

Start time:	09:43:27
Start date:	01/11/2021
Path:	/tmp/V2WzER53Tt
Arguments:	n/a
File size:	71312 bytes
MD5 hash:	4b0259083c8800d18cb941c66639a2e6

Analysis Process: V2WzER53Tt PID: 5244 Parent PID: 5242

General

Start time:	09:43:27
Start date:	01/11/2021
Path:	/tmp/V2WzER53Tt
Arguments:	n/a
File size:	71312 bytes
MD5 hash:	4b0259083c8800d18cb941c66639a2e6

File Activities

File Read

Directory Enumerated

Analysis Process: V2WzER53Tt PID: 5245 Parent PID: 5242

General

Start time:	09:43:27
Start date:	01/11/2021
Path:	/tmp/V2WzER53Tt
Arguments:	n/a
File size:	71312 bytes
MD5 hash:	4b0259083c8800d18cb941c66639a2e6